4 二重化構成について

本章ではFirewallServerを2台使用して、二重化構成を構築するための手順について説明します。

概　要

二重化構成について説明します。

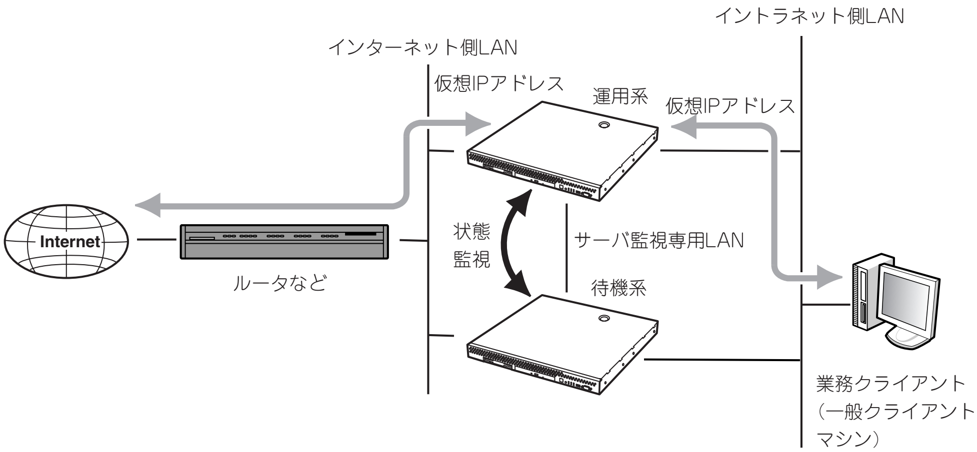
動作概要

FirewallServerを二重化することで1台が障害などにより停止しても、もう1台のサーバへ自動的に引き継ぐことにより、障害時の業務停止時間を最小限に抑えることができます。

また、運用系でFireWall-1プロセスの異常を検出した場合、および設定されたIPアドレスとの通信が途絶した場合にも、待機系に業務を引継ぐことが可能です。

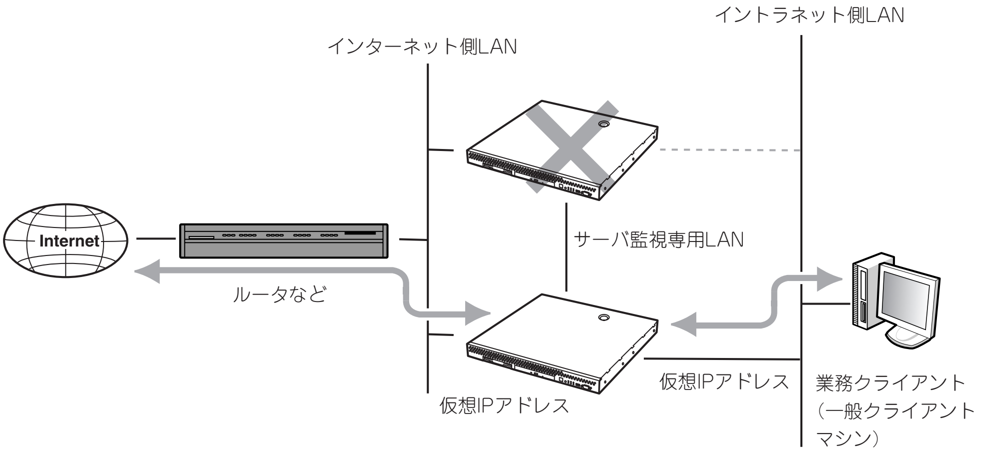
以下の仕組みでFirewallServerを二重化します。

- **通常運用時**
  - 運用系側のFirewallServerで有効にした仮想IPアドレスを使用してインターネット側、イントラネット側の双方からアクセスします。
  - 運用系/待機系のFirewallServerは互いにサーバの状態を監視をします。



● **運用系サーバダウン時**

- 待機系のFirewallServerが運用系のダウンを検出します。
- 待機系のFirewallServerが仮想IPアドレスを有効にします。
- インターネット側、イントラネット側の双方からのアクセスは仮想IPアドレスを使用しているのでサーバの切り替わりを意識することはありません。



DMZを使用する場合もイントラネット、インターネット同様に仮想IPアドレスが引き継がれます。

構　成

二重化構成ではFirewallServer2台のほかに管理用サーバ（Windows NT Serverなど）が1台必要になります。
管理用サーバにFireWall-1管理モジュールをインストールし、2台のFirewallServerを管理します。

必要なリソース

二重化を実現するためにはFirewallServerを単体で運用するときに比べて新たなリソースが必要です。
セットアップの前にリソースの計画や設定をしてください。

- **仮想IPアドレス(インターネット側): 1つ**

  インターネット側で引き継ぐアドレスです。

  インターネット側のネットワークアドレス内で未使用のホストアドレスをアサインしてください。

  このアドレスはサーバに設定する必要はありません。

- **仮想IPアドレス(イントラネット側): 1つ**

  イントラネット側で引き継ぐアドレスです。

  イントラネット側のネットワークアドレス内で未使用のホストアドレスをアサインしてください。

  このアドレスはサーバに設定する必要はありません。

- **仮想IPアドレス(DMZ側): 1つ**

  DMZで引き継ぐアドレスです。

  DMZを設けない場合には不要です。

  DMZのネットワークアドレス内で未使用のホストアドレスをアサインしてください。

  このアドレスはサーバに設定する必要はありません。

- **サーバ間通信用アドレス: 1つ、もしくは2つ**

  FirewallServer間の監視に使用するアドレスです。

  インターネット側、イントラネット側と共用にしても問題はありませんが、可能であれば、専用のポートを使用してください。

  専用のポートが用意できる場合、サーバ間をクロスケーブルで接続してください。

  それぞれのサーバに最低一つずつ設定してください。

設定手順

以下のネットワーク構成を例にとって設定を行います。

- **運用系サーバ**

ホスト名:	fws1
インターネット側実IPアドレス:	202.247.5.1/255.255.255.0
DMZ側実IPアドレス:	172.16.1.1/255.255.255.0
イントラネット側実IPアドレス:	192.168.1.1/255.255.255.0
サーバ間通信用IPアドレス:	192.168.2.1/255.255.255.0

- **待機系サーバ**

ホスト名:	fws2
インターネット側実IPアドレス:	202.247.5.2/255.255.255.0
DMZ側実IPアドレス:	172.16.1.2/255.255.255.0
イントラネット側実IPアドレス:	192.168.1.2/255.255.255.0
サーバ間通信用IPアドレス:	192.168.2.2/255.255.255.0

- **仮想IPアドレス**

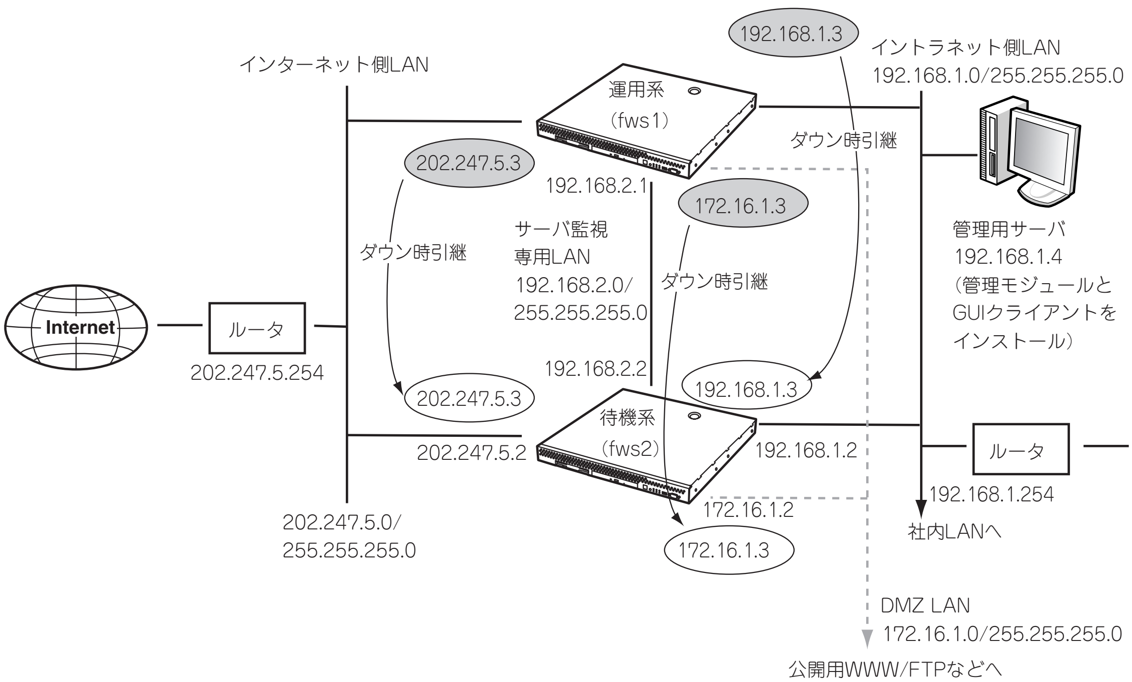
インターネット側:	202.247.5.3
DMZ側:	172.16.1.3
イントラネット側:	192.168.1.3

- **監視先IPアドレス**

インターネット側ルータ:	202.247.5.254
イントラネット側ルータ:	192.168.1.254

- **管理用サーバ**

ホスト名:	firewall_mgr
IPアドレス:	192.168.1.4/255.255.255.0



セットアップの流れ

以下にセットアップの流れを示します。ここでは二重化に関する設定内容のみを説明します。その他の手順については第2章の「セットアップ」を参照してください。

管理用コンピュータのセットアップと接続 →第2章の51ページ

↓

FireWall-1管理サーバのセットアップ →119ページ〜123ページ

↓

FirewallServerのセットアップ

1. マシンの基本設定 →第2章の54ページ〜57ページ

↓

2. FireWall-1モジュールのインストール →第2章の58ページ

↓

3. FireWall-1のコンフィグレーション →124ページ〜126ページ

↓

セキュリティポリシーの設定 →127ページ

↓

二重化機能の基本設定 →133ページ

↓

他のネットワーク機器の設定 →138ページ

FireWall-1管理サーバのセットアップ

二重化する2台のFirewallServerを管理するための管理サーバをセットアップします。以下の条件を満たすコンピュータに管理モジュールをインストールしてください。

オペレーティングシステム:	Windows NT 4.0 Server (SP6a)、 Windows 2000 Server (SP1、 SP2)、 Windows 2000 Advanced Server (SP1、 SP2)、 Solaris/SPARC 7 (32bit)、 Solaris/SPARC 8 (32bit、 64bit)、 RedHat Linux 6.2 (kernel version 2.2.14、 2.2.17)、 RedHat Linux 7.0 (kernel version 2.2.16、 2.2.17、 2.2.19)、 RedHat Linux 7.2 (kernel version 2.4.9-13)
ディスク容量:	40MB以上
メモリ:	256MB以上推奨

* 上記は2002年3月現在の情報です。今後のパッチリリースにより変更になる可能性があります。

以下は1台のWindows 2000 Serverに管理モジュールとGUIクライアントをインストールする場合の設定例です。

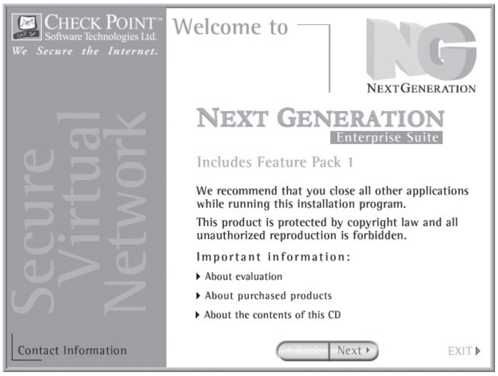
管理モジュールとGUIクライアントのインストール

1. コンピュータのCD-ROMドライブにCheck Point Next GenerationのCD-ROMをセットする。

   自動的にインストールプログラムが起動し、画面が表示されます。
   インストールプログラムが起動しない場合は¥wrappers¥windowsフォルダにある「demo32.exe」を実行してください。

2. [Next]をクリックする。

   使用許諾契約書が表示されます。



3. 内容をよく読み、同意する場合は[Yes]をクリックする。

   同意しない場合は[No]をクリックして終了します。
   プロダクトメニューの画面が表示されます。

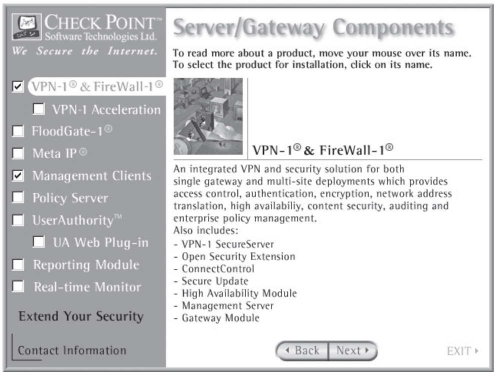
4. 「SERVER/GATEWAY COMPONENTS」を選択し、[Next]をクリックする。

   プロダクト選択の画面が表示されます。

5. 「VPN-1 & FireWall-1」と「Management Clients」をチェックして、[Next]をクリックする。

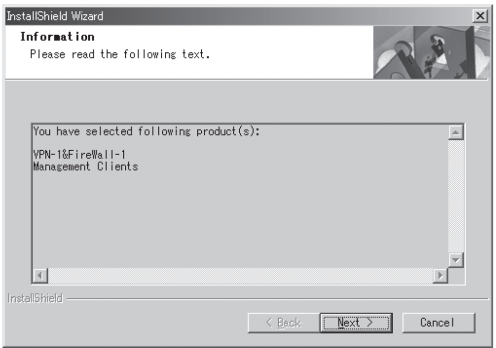
   チェック

   その他のコンポーネントのチェックは外します。



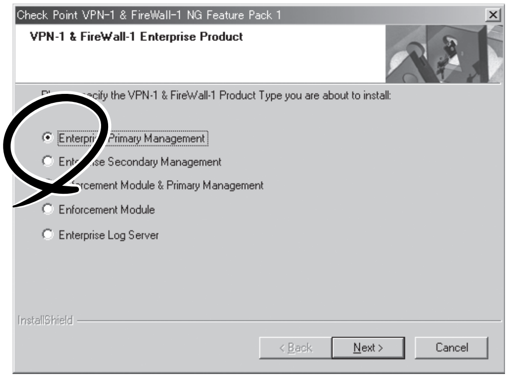
6. 右図の内容が表示されていることを確認し、[Next]をクリックする。

   インストールするコンポーネントを選択する画面が表示されます。



7. 「Enterprise Primary Management」をチェックして、[Next]をクリックする。

旧バージョンのVPN-1/FireWall-1モジュールを管理するかを選択する画面が表示されます。



8. 「Install without backward compatibility」をチェックして、[Next]をクリックする。

「VPN-1 & FireWall-1」インストール先のフォルダを指定する画面が表示されます。

9. 必要に応じてフォルダを変更し、[Next]をクリックする。

インストールが開始されます。

10. インストール完了メッセージが表示されたら[OK]をクリックする。

「Management Clients」インストール先のフォルダを指定する画面が表示されます。

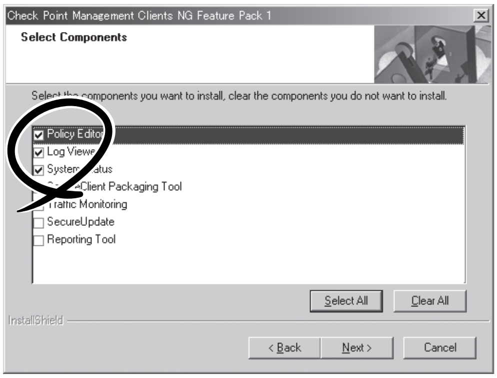
11. 必要に応じてフォルダを変更し、[Next]をクリックする。

インストールするコンポーネントを選択する画面が表示されます。

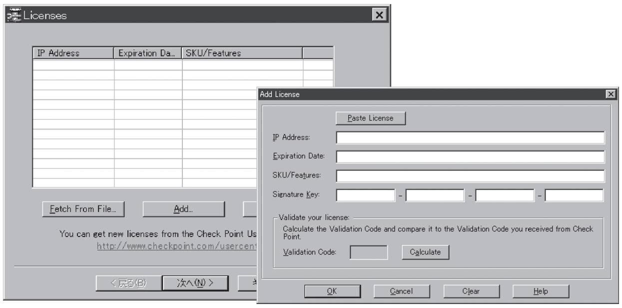
12. 「Policy Editor」、「Log Viewer」、「System Status」にチェックして[Next]をクリックする。

インストールが開始されます。

13. インストール完了メッセージが表示されたら[OK]をクリックする。

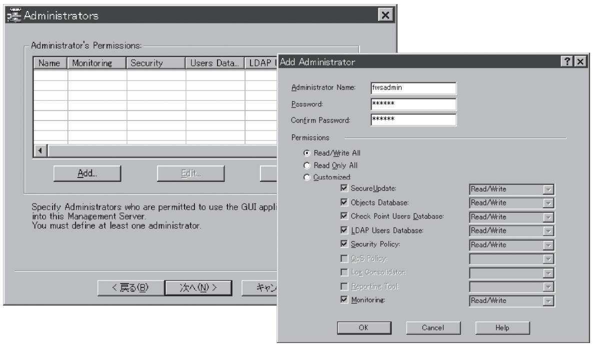


引き続きFireWall-1のコンフィグレーションを行います。
最初にライセンスの入力画面が表示されます。



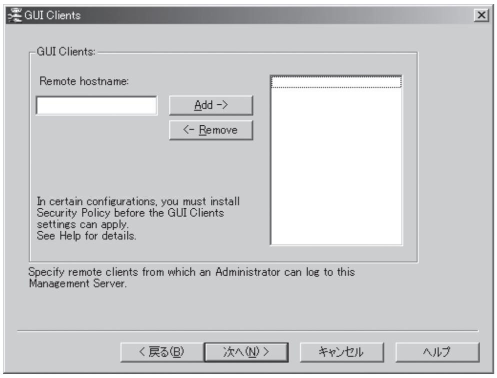
14. [Fetch From File]をクリックしてライセンスが送付されてきたE-mailの添付ファイル(*.lic)を指定するか、[Add]をクリックし、取得したライセンス情報を入力する。

管理者の設定画面が表示されます。



15. [Add]をクリックし、FireWall-1の管理者、パスワード、および属性を設定する。

GUIクライアントの設定画面が表示されます。



本構築例ではGUIクライアントを管理サーバと同一のコンピュータにインストールするので設定は必要ありません。GUIクライアントを別コンピュータにインストールする場合には、そのコンピュータのIPアドレスを設定してください。

ランダムキーを入力する画面が表示されます。

16. バーがフルになるまで入力する。

Certificate Authorityが作成されます。

17. 設定が完了したらコンピュータを再起動させる。



FireWall-1のコンフィグレーション

二重化構成の場合、コンフィグレーション手順が第2章の「セットアップ」とは一部異なります。次の手順に従ってコンフィグレーションを行います。
設定はFireWall-1付属のcpconfigコマンドで行います。

```
# cpconfig

Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue......................................................................................................... ①
                :
                :
                :
Do you accept all the terms of this license agreement (y/n) ? y ...................................... ②

which Module would  you like to install?
-------------------------------------------
(1) VPN-1 & FireWall-1 Enterprise Primary Management and Enforcement Module
(2) VPN-1 & FireWall-1 Enforcement Module
(3) VPN-1 & FireWall-1 Enterprise Primary Management
(4) VPN-1 & FireWall-1 Enterprise Secondary Management
(1) VPN-1 & FireWall-1 Enterprise Log Server

Enter your selection (1-5/a):2 ...................................................................................... ③

In this a Dynamically Assigned IP Address Module instaration? (y/n) [n] ? n ..................... ④

Would you like to install the High Availability product? (y/n) [n] ? y ........................... ⑤
```

① <Enter>キーを押す。

使用許諾書が表示されますのでお読みください。

② 使用許諾に承認した場合は<Y>キーを押す。

③ インストールするモジュールを選択する。

二重化構成の場合は2を選択し、分散型構成でインストールします。

④ Dynamically Assigned IP Address Moduleをインストールするか問い合わせがあるので、<N>キーを押す。

⑤ High Availability productをインストールするか問い合わせがあるので、<Y>キーを押す。

```
Configuring Licenses...
=============================
Host            Expiration Features

Do you want to add licenses (y/n) [n] ? y ............ ①

Do you want to add licenses [M]anually or [F]etch from file: m ............ ②
IP Address:202.247.5.1
Expiration Date:
Signature Key:                           ............ ③
SKU/Features:

License was added successfully

License will be put into kernel after cpstart

Configuring Groups...
=====================
VPN-1 & FireWall-1 access and execution permissions
-------------------------------------------
Usually, a VPN-1 & FireWall-1 module is given group permission
for access and execution.
You may now name such a group or instruct the installation
procedure to give no group permissions to the VPN-1 & FireWall-1 module.
In the latter case, only the Super-User will
be able to access and execute the VPN-1 & FireWall-1 module.

Please specify group name [<RET> for no group permissions]: ............ ④

No group permissions will be granted. Is this ok (y/n) [y] ? y ............ ⑤

Setting Group Permissions... Done.
```


① <Y>キーを入力して、ライセンスを追加する。

② <M>キーを入力して、ライセンスを画面から(マニュアルで)入力する。

③ 事前に取得したライセンス情報を入力する。

④ FirewallServerでは通常グループを作成しないので<Enter>キーを押して続ける。

⑤ <Y>キーを押して続ける。

```
Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used in
various cryptographic operations.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [....................] ........................................ ①

Thank you.

Configuring Secure Internal Communication...
============================================
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Uninitialized
Enter One Time Password: ┐
Again One Time Password: ┘............................................. ②

The Secure Internal Communication was successfully initialized

initial_module:
Compiled OK.

Hardening OS security: Initial policy will be applied
until the first policy is installed

In order to complete the installation of module
you must reboot the machine.
Do you want to reboot? (y/n) [y] ? y ..................................③
```

① バーがフルになるまでランダムキー入力をする。

② FireWall-1管理サーバとFirewallServer間での通信に使用するパスワードを設定する。

③ 終了後、再起動する。

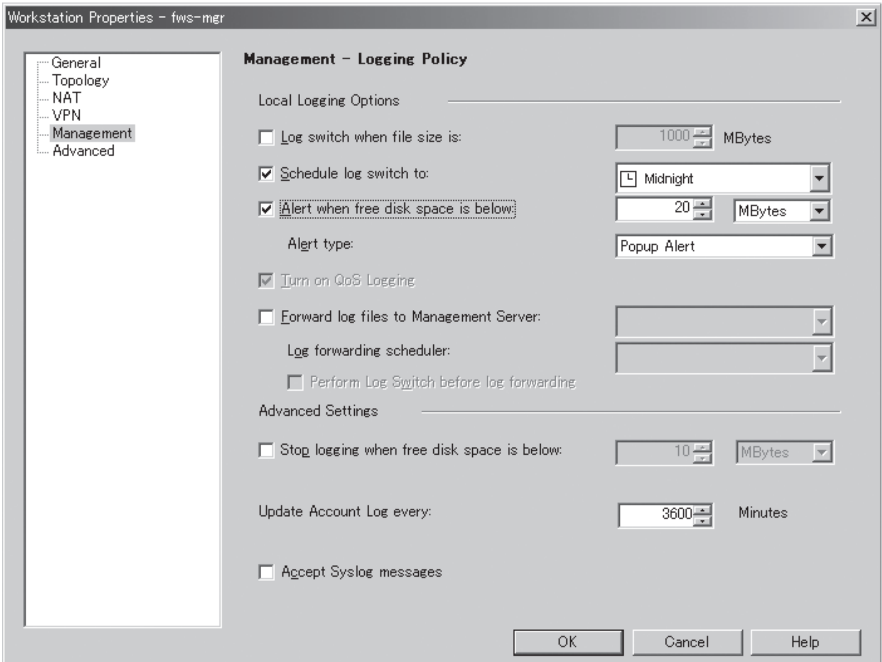
セキュリティポリシーの設定

FireWall-1管理サーバ上でセキュリティポリシーを作成し、管理対象の2台のFirewallServerに同時にインストールします。

ログファイルローテーションの設定

二重化構成ではFireWall-1管理サーバにログを保存するために、以下の手順でログファイルのローテーション設定を行います。
FireWall-1管理サーバのオブジェクト（最初にPolicy Editorを起動するとFireWall-1管理サーバのオブジェクトが自動的に生成されます。）を開き、Managementページで「Schedule log switch to:」にチェックし切り替え時間を設定します。

重要 **上記設定でログファイルのローテーションは実行されますが、ファイルは削除されません。空きディスク容量をチェックして、古いログファイルを手動で削除するようにしてください。**



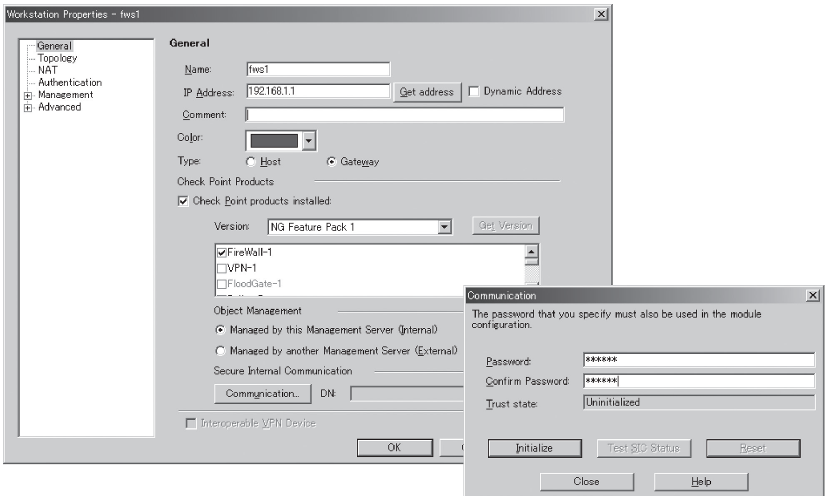
Firewall Gatewayオブジェクトの作成

二重化構成ではFirewall Gateway(FirewallServer)のオブジェクトの作成方法が異なります。

1. 2台のFirewallServerのオブジェクトを作成する。

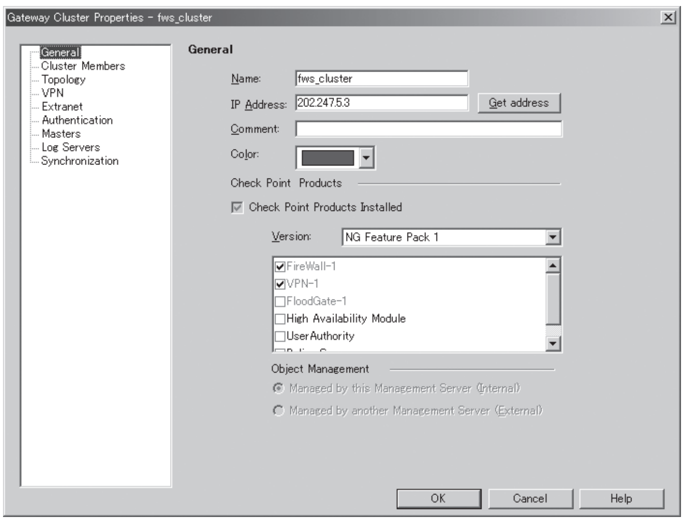
   オブジェクト：Workstation
   名前　　　　：fws1、fws2
   内容　　　　：IP Address にはFireWall-1管理サーバと同じネットワーク（イントラネット）の実IPアドレスを指定する
   Topologyページで全インタフェースを設定する。

   FireWall-1管理サーバからFirewallServerを管理（セキュリティポリシーの設定やログ表示など）するためには、FireWall-1管理サーバとFirewallServerとの間で通信を行うための設定が必要です。Generalページで[Communication...]をクリックし、FireWall-1のコンフィグレーション時に設定したパスワードを入力します。

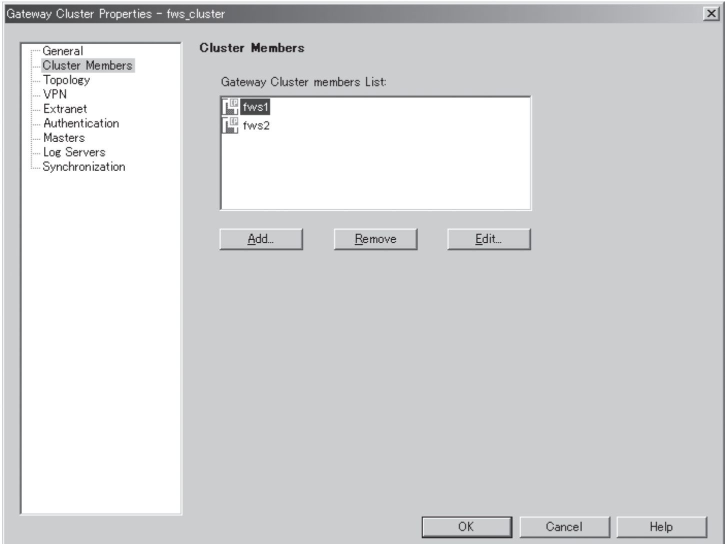


2. ネットワークオブジェクトとして以下のオブジェクトを作成する。

   オブジェクト：Gateway Cluster
   名前　　　　：fws_cluster
   内容　　　　：IP Addressにはインターネット側の仮想IPアドレスを指定する



3. Cluster Membersページで、手順1で作成した2台のFirewallServerオブジェクト(fws1、fws2)を追加する。

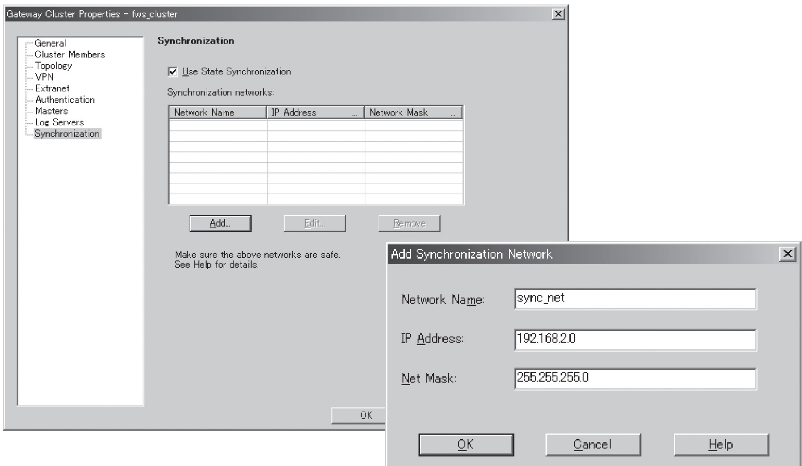


4. Synchronizationページで同期を実行するネットワークを入力する。

同期を行うことにより、運用系サーバ(fws1)が停止し、待機系サーバ(fws2)が代わりに起動した場合にfws2は、fws1で接続の更新された状態を保持するため、接続を維持することができます。

チェック

異なるコンピュータで実行しているVPN-1 ／FireWall-1モジュールは、互いの状態を同期することができ、これにより情報を共有し、接続の状態が変更される毎に互いの情報を更新することができます。

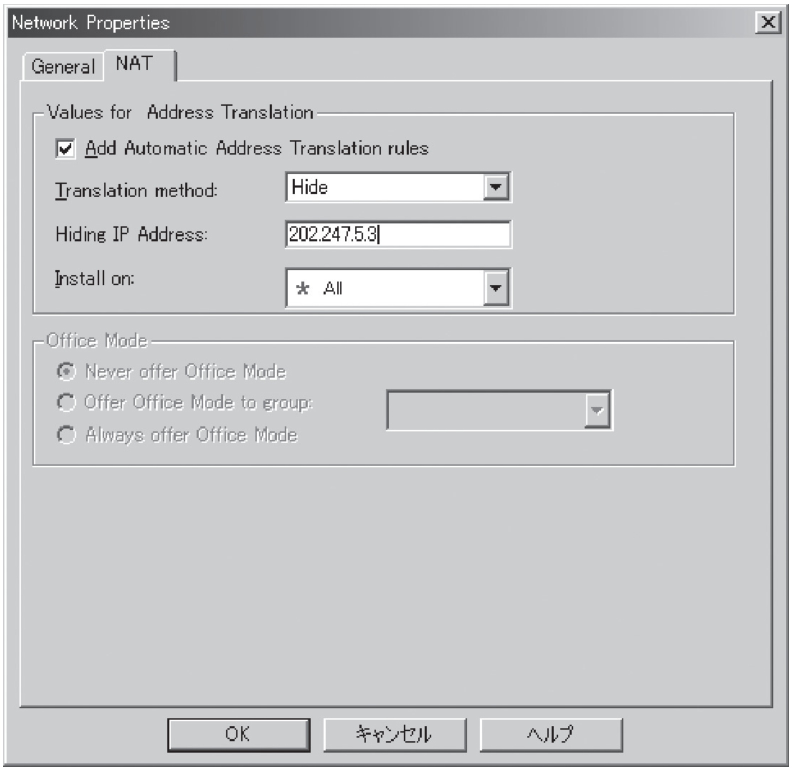


二重化構成について

セキュリティポリシーの作成

ネットワーク構成に応じてセキュリティポリシーを作成してください。
ステルスルール(FirewallServer自身へのアクセスを拒否するルール)に関してはfws1、fws2の両サーバを設定することに注意してください。

ネットワークに対してHideモードのNATを設定する場合、Hiding IP Addressにはインターネット側の仮想IPアドレスを指定します。

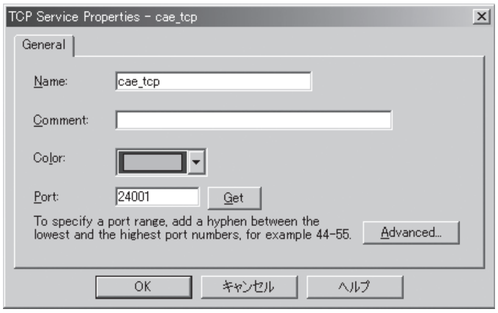


二重化用ルールの追加

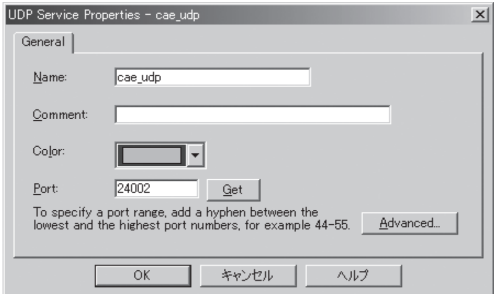
二重化機能を使用するためには、FirewallServer間の状態監視用通信を通すためのルールを設定する必要があります。

1. 以下のサービスを定義します。(名前は一例です。他の名前でも構いません。)

オブジェクト:TCP
名前　　　:cae_tcp
ポート　　:24001



オブジェクト:UDP
名前　　　:cae_udp
ポート　　:24002



重要

上記ポート番号はデフォルトのポート番号です。二重化機能の基本設定でポート番号を変更する場合はその設定に合わせてサービスの定義を行ってください。

2. 二重化通信用のルールを追加する。

ルールセットの一番上にくるように追加してください。(下記ポリシーのNO. 1)

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	fws1 fws2	fws1 fws2	cae_tcp cae_udp	accept	None	Gateways	Any	
2	Any	fws1 fws2	Any	drop	Alert	Gateways	Any	Stealth the Firewall att
3	LocalNet	MailServer	pop-3	accept	Log	Gateways	Any	Local network e-mail r
4	Any	MailServer	smtp	accept	Log	Gateways	Any	Incoming mail access t
5	MailServer	Any	smtp	accept	Log	Gateways	Any	Outgoing mail from the
6	Any	WebServer	http ftp	accept	Log	Gateways	Any	Open access to the w
7	DMZnet	LocalNet	Any	reject	Alert	Gateways	Any	Protect the local netwo
8	LocalNet	DMZnet	Any	reject	Alert	Gateways	Any	Protect the DMZ netwo
9	LocalNet	Any	InternetServices	accept	Log	Gateways	Any	Allow Selective Outgoi
10	Any	Any	SilentServices	drop	None	Gateways	Any	Silent drop for broadca
11	Any	Any	Any	drop	Alert	Gateways	Any	Last rule

セキュリティポリシーのインストール

セキュリティポリシーの作成が完了したら、ポリシーをインストールしてください。2台のFirewallServerに一度にインストールされます。

セキュリティポリシーのバックアップ

二重化構成の場合、FireWall-1管理サーバにポリシー情報が保存されます。何らかの要因でFireWall-1管理サーバを再インストールする場合にそなえて以下のディレクトリ配下の全ファイルをバックアップしてください。

$FWDIR¥conf\配下
$FWDIR¥database\配下
$FWDIR¥lib\配下
($FWDIRはFireWall-1をインストールしたディレクトリ、通常はC:¥WINNT¥FW1¥NG)

二重化機能の基本設定

二重化機能の基本設定方法を説明します。設定は基本設定ツールから行います。両サーバで全く同じ設定を行ってください。
二重化機能の設定項目およびそれぞれの制限事項は以下のとおりです。

- **ハートビート送信間隔**

  サーバ監視用のパケット送信間隔(秒)を入力します。デフォルトは1(秒)です。

- **ハートビートタイムアウト時間**

  ハートビートが途絶して相手サーバがダウンしたと認識するまでの時間(秒)を指定します。ハートビート送信間隔より大きい値を指定してください。デフォルトは5(秒)です。

- **内部通信用TCPポート番号**

  2台のFirewallServer間で通信を行うためのTCPのポート番号を指定します。

- **内部通信用UDPポート番号**

  2台のFirewallServer間で通信を行うためのUDPのポート番号を指定します。

- **サーバ1のホスト名**

  ホスト名はFQDN形式ではなく、ドメイン名部分を除いた名前を指定してください。

- **サーバ2のホスト名**

  ホスト名はFQDN形式ではなく、ドメイン名部分を除いた名前を指定してください。

- **サーバ1のインタコネクトアドレス**

  相手サーバを監視するためのアドレスとネットマスクを入力します。

- **サーバ2のインタコネクトアドレス**

  相手サーバを監視するためのアドレスとネットマスクを入力します。

- **仮想IPアドレス**

  二重化機能を使用する場合、FirewallServerへのアクセスは原則仮想IPアドレスを使用する必要があります。

  サーバ間監視専用インタフェースを除く全インタフェースに仮想IPアドレスを設定してください。

- **監視対象IPアドレス**

  監視対象として設定されたIPアドレスとの通信が途絶した場合、待機系サーバにフェイルオーバが行われます。

- **運用系サーバ**

  サーバ1とサーバ2のどちらを運用系サーバにするかを指定します。

- **自動フェイルバック**

  自動フェイルバックを行うかどうか設定します。自動フェイルバックをautoにした場合、運用系ダウン後、待機系に業務が引き継がれている状態で、運用系が復帰(起動)すると、自動的に運用系に業務を戻します。

以下に基本設定ツールでの設定手順を示します。

```
# /opt/necfws/bin/fwsetup ……………………………………………… ①
Firewall Server configuration tool Ver.1.4
            <省略します。2章の「セットアップ」を参照してください。>
use cluster system? (y/n)[y]: y ……………………………………… ②
---- START CLUSTERPRO AE configuration ---------------
CLUSTERPRO AE Configuration Tool Ver 1.1
---- cluster configuration ---------------------------
Input HB interval(1 - 999)[1] : ……………………………………… ③
Input HB timeout(1 - 999)[5] : ………………………………………… ④
Input API TCP port number[24001] : ………………………………… ⑤
Input HB UDP port number[24002] : …………………………………… ⑥
Input server1 host name : fws1 ………………………………………… ⑦
Input server2 host name : fws2 ………………………………………… ⑧
```

① 設定ツールを起動する。

② 二重化機能を使用するかの問い合わせがあるので、<Y>キーを押す。

③ ハートビート送信間隔を入力する。

④ ハートビートタイムアウト時間を入力する。

⑤ 内部通信用のTCPポート番号を入力する。

⑥ 内部通信用のUDPポート番号を入力する。

⑦ サーバ1のホスト名を設定する。
ホスト名はFQDN形式ではなく、ドメイン名部分を除いた名前を指定してください。

⑧ サーバ2のホスト名を設定する。
ホスト名はFQDN形式ではなく、ドメイン名部分を除いた名前を指定してください。

```
---- server configuration ---------------------------

Input fws1 interconnect address ..................................................①
address(1) : 192.168.2.1
netmask(1) : 255.255.255.0
address(2) : 192.168.1.1
netmask(2) : 255.255.255.0
address(3) :
 No.  address/netmask
  1   192.168.2.1/255.255.255.0
  2   192.168.1.1/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

Input fws2 interconnect address ..................................................②
address(1) : 192.168.2.2
netmask(1) : 255.255.255.0
address(2) : 192.168.1.2
netmask(2) : 255.255.255.0
address(3) :
 No.  address/netmask
  1   192.168.2.2/255.255.255.0
  2   192.168.1.2/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 運用系サーバのサーバ間監視用アドレス(インタコネクトアドレス)とネットマスクを入力する。

サーバ間監視用アドレス(インタコネクトアドレス)は2個まで設定可能です。

設定後に一覧を表示します。

一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

<A>キー + <Enter> キー:	インタコネクトアドレスを追加します。
<M>キー+「修正する一覧の番号」+<Enter>キー:	指定した番号の設定を修正します。
<D>キー+「削除する一覧の番号」+<Enter>キー:	指定した番号の設定を削除します。
<L>キー+<Enter>キー:	一覧を再表示します。
<Enter>キー:	次の項目へスキップします。

② 待機系サーバのサーバ間監視用アドレス(インタコネクトアドレス)とネットマスクを入力する。

運用系サーバの場合と同様に一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

```
---- fip configuration -----------------------------

Input FIP address ······························ ①
address(1) : 202.247.5.3
netmask(1) : 255.255.255.0
address(2) : 172.16.1.3
netmask(2) : 255.255.255.0
address(3) : 192.168.1.3
netmask(3) : 255.255.255.0
address(4) :
 No.  address/netmask
  1   202.247.5.3/255.255.255.0
  2   172.16.1.3/255.255.255.0
  3   192.168.1.3/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 仮想IPアドレスを入力する。

仮想IPアドレスは8個まで設定可能です。

設定後に一覧を表示します。

一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

<A>キー + <Enter> キー:	仮想IPアドレスを追加します。
<M>キー+「修正する一覧の番号」+<Enter>キー:	指定した番号の設定を修正します。
<D>キー+「削除する一覧の番号」+<Enter>キー:	指定した番号の設定を削除します。
<L>キー+<Enter>キー:	一覧を再表示します。
<Enter>キー:	次の項目へスキップします。

ヒント

二重化機能を使用する場合、FirewallServerへのアクセスは、原則仮想IPアドレスを使用する必要があります。
サーバ間監視専用インタフェース以外の全インタフェースに仮想IPアドレスを設定してください。

```
---- ipw configuration ------------------------------

Input IPW address address ..................................................... ①
address(1) : 202.247.5.254 |202.247.5.5
address(2) : 192.168.1.254
address(3) :
 No.  address
  1   202.247.5.254 |202.247.5.5
  2   192.168.1.254

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 監視するIPアドレスを入力する。

「|」で区切って複数のIPアドレスを入力することができます。その場合は、指定した全IPアドレスとの通信が途絶した場合にリソース異常となります。

監視するIPアドレスは8個まで設定可能です。ただし、「|」で区切ったIPアドレスは全体で1つのIPアドレスとしてカウントします。

設定後に一覧を表示します。一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

<A>キー + <Enter> キー:	監視するIPアドレスを追加します。
<M>キー+「修正する一覧の番号」+<Enter>キー:	指定した番号の設定を修正します。
<D>キー+「削除する一覧の番号」+<Enter>キー:	指定した番号の設定を削除します。
<L>キー+<Enter>キー:	一覧を再表示します。
<Enter>キー:	次の項目へスキップします。

ヒント

監視対象として設定されたIPアドレスとの通信が途絶した場合、待機系サーバにフェイルオーバが行われます。

<設定例>

- 202.247.5.254と192.168.1.254のどちらかと通信が途絶した場合にフェイルオーバを行いたい場合。

No.	address
1	202.247.5.254
2	192.168.1.254

- 202.247.5.254と192.168.1.254の双方と通信が途絶した場合にフェイルオーバを行いたい場合。

No.	address
1	202.247.5.254 | 192.168.1.254

- 202.247.5.5と202.247.5.254の双方と通信が途絶した場合か、192.168.1.254と通信が途絶した場合にフェイルオーバを行いたい場合

No.	address
1	202.247.5.5 | 202.247.5.254
2	192.168.1.254

```
---- resource configuration -------------------------

Input primary server hostname(fws1, fws2)[fws1] : ............ ①

Input failback policy(1:auto, 2:manual)[manual] : ............ ②

---- END CLUSTERPRO AE configuration ----------------- ........ ③

once again input? (y/n)[n]:

change root password? (y/n)[n]:

Thu May 17 20:21:50 JST 2001
set date and time? (y/n)[n]:


stop unnecessary services? (y/n)[n]:

Please reboot the system.

# shutdown -r now ............................................ ④
```

① 運用系サーバを入力する。

② 自動フェイルバックを行うかどうか入力する。

自動フェイルバックをautoにした場合、運用系ダウン後、待機系に業務が引き継がれている状態で、運用系が復帰（起動）すると、自動的に運用系に業務を戻します。

③ 二重化機能の設定の終了。

④ 設定を有効にするため、再起動する。

他のネットワーク機器の設定

イントラネットとDMZに存在するネットワーク機器については、デフォルトルートの設定としてそれぞれのネットワークの仮想IPアドレス（イントラネット側: 192.168.1.3、DMZ側: 172.16.1.3）を指定するようにしてください。

運　用

二重化構成の運用について説明します。

障害発生時の対応

運用系サーバにおいて障害を検出した場合には、フェイルオーバが発生し待機系サーバへ業務が切り替わります。その際に基本設定ツールで指定した管理者のE-mailアドレス宛にメールが送信されます。

● ダウンしたときのメッセージ

```
Subject: WARNING: Firewall is downed

 !!WARNING!!
 Firewall(fws1.nec.co.jp[202.247.5.1]) is not active.
 Urgently check it.

 If you recieved a previous message "NOTICE: Switch over to
 the active firewall" from fws1.nec.co.jp[202.247.5.1],
 both firewalls are downed.
 Urgently check both firewalls!!
```

● フェイルオーバしたときのメッセージ

```
Subject: NOTICE: Switch over to the active firewall

 !!NOTICE!!
 Switch over to the active firewall(fws2.nec.co.jp[202.247.5.2]).
 Urgently check another failed firewall.
```

重要

ダウンした要因がネットワークの通信障害などの場合、ダウンしたときのメッセージがFirewallServer内に滞留し、障害復旧後に送信されることがあります。メッセージを受信したら必ずその発信時刻を確認するようにしてください。

メールを受信したらFirewallServerの状態を確認し、システムログ(syslog)からフェイルオーバが発生した要因を確認し、必要な対処を行ってください。メッセージ内容、対処方法等は「付録C 二重化機能のログメッセージ」(262ページ)を参照してください。

監視対象IPアドレスとの通信途絶、あるいは、FireWall-1プロセス異常が発生し、待機系サーバに業務を引き継いだ場合、以後、そのサーバ上での業務の起動が拒否されるようになります。そのサーバが業務の起動拒否状態かどうかは、[caestat-i]コマンドの[ENVIRONMENT]で確認できます。[ENVIRONMENT]が "DEACT_ILLEGAL" の場合は起動拒否状態となっていることを表します。
起動拒否状態となっている場合は速やかにその障害の対処を行い、サーバの再起動を行ってください。

コマンドリファレンス

状態表示、運用系、待機系の切替等はコマンドを使用して行います。

情報表示

現在の状態、設定内容を確認するには以下のコマンドを実行します。

caestat -s [-h host_name]
-i [-h host_name]

状態、設定情報の表示を行います。

-sまたは引数なし .... 各種状態を表示します。
-i.................................. 各種設定を表示します。
-h host_name .... 操作対象サーバ名。指定なしの場合、コマンド実行サーバが対象となります。

```
# caestat -s

--------------------------------------------------
 CLUSTER STATUS on fws1
--------------------------------------------------

 SERVER: host1                 ONLINE  .......... ①
   GROUP: group0               ONLINE  .......... ②
     RESOURCE: fip0            ONLINE  .......... ③
     RESOURCE: fip1            ONLINE
     RESOURCE: ipw0            ONLINE
     RESOURCE: ipw1            ONLINE
     RESOURCE: exec0           ONLINE
     RESOURCE: exec1           ONLINE
     RESOURCE: exec2           ONLINE

 SERVER: host2                 ONLINE
   GROUP: group0               OFFLINE
     RESOURCE: fip0            OFFLINE
     RESOURCE: fip1            OFFLINE
     RESOURCE: ipw0            OFFLINE
     RESOURCE: ipw1            OFFLINE
     RESOURCE: exec0           OFFLINE
     RESOURCE: exec1           OFFLINE
     RESOURCE: exec2           OFFLINE
```

① サーバの状態

② グループの状態

③ 各リソースの状態

```
# caestat -i

-------------------------------------------------
 CLUSTER INFORMATION on fws1
-------------------------------------------------

 CLUSTER :
  STARTUP              : AUTO ········· ①
  HB interval          : 1 ············ ②
  HB timeout           : 5 ············ ③
  WAIT timeout         : 5
  HB port              : 24002 ········ ④
  API port             : 24001 ········ ⑤
  API timeout          : 30
  ping timeout         : 1
  RECOVER              : RESTART
  RETRY count          : 5

  SERVER0 : host1 ····················· ⑥
   INTERCONNECT0       : 192.168.1.1/255.255.255.0 ····· ⑦
   INTERCONNECT1       : 192.168.2.1/255.255.255.0

  SERVER1 : host2
   INTERCONNECT0       : 192.168.1.2/255.255.255.0
   INTERCONNECT1       : 192.168.2.2/255.255.255.0

   GROUP0 : group0
    START              : AUTO
    FAILBACK           : MANUAL ······· ⑧
    ENVIRONMENT        : ACT_NORMAL
    RECOVER            : IGNORE
    RETRY count        : 0
    FAILOVER policy    : host1 host2 ·· ⑨

    FIP0 : fip0
     ADDRESS           : 202.247.5.3/255.255.255.0 ····· ⑩
     INTERFACE         : eth0:0
     PING count        : 0
     ARP count         : 1
     RECOVER           : RETRY
     RETRY count       : 5

    IPW0 : ipw0
     POLLING address : 202.247.5.254 | 192.168.1.254 ··· ⑪
     RECOVER           : FAILOVER
     RETRY count       : 2
```

① 二重化機能が有効になっているかどうか

② ハートビート送信間隔(秒)

③ ハートビートタイムアウト時間(秒)

④ 内部通信用UDPポート番号

⑤ 内部通信用TCPポート番号

⑥ ホスト名

⑦ インタコネクトアドレス

⑧ 自動フェイルバックを行うかどうか

⑨ 運用系サーバ 待機系サーバ

⑩ 仮想IPアドレス

⑪ 監視対象アドレス

運用系／待機系の切り替え・業務の起動／停止

運用系／待機系の切替や、業務の起動／停止を行う場合、以下のコマンドを実行します。

```
caegrp -s  [-h host_name]
       -t  [-h host_name]
       -m  [-h host_name]
```

業務の起動／停止関連操作を行います。

-s .... 業務の起動を行います。すでに起動されていたり、他のサーバで起動している場合には失敗します。

-t .... 業務の停止を行います。すでに停止されていたり、他のサーバで起動されている場合には失敗します。

-m .... 業務の実行サーバを切り替えます。業務が起動しているサーバ側で実行する必要があります。

-h host_name .... 操作対象サーバ名です。指定なしの場合、コマンド実行サーバが対象となります。-m オプション指定時には、業務移動元サーバの意味も持ちます。

二重化構成の再セットアップ

二重化構成の場合の再セットアップについて説明します。
次の手順に従ってFairewallServerを再インストールします。

1. 「システムの再インストール」(77ページ)を参照しながら手順10までを行う。
2. 続いて、「FireWall-1のコンフィグレーション」(124ページ)の作業を行う。
3. 管理サーバのPolicy Editorで、再セットアップを行ったFirewallServerのFirewall Gatewayオブジェクトの Workstation Propertiesウィンドウを開く。

   Generalタブの[Communication...]をクリックし、FireWall-1モジュールのインストール時に設定したパスワードを再入力します。(再セットアップ前と同じパスワードを設定した場合でも必ず再入力してください。)

4. セキュリティポリシーを再インストールする。

二重化構成の場合はセキュリティポリシーがFireWall-1管理サーバの中に保存されているため、FirewallServer本体の再インストールの際にはFireWall-1ポリシー情報のリストアは必要ありません。

重要 **FireWall-1管理サーバを再インストールする場合には「セキュリティポリシーのバックアップ」(132ページ)でバックアップしておいたファイルをリストアしてください。**

注意・制限事項

- FirewallServerは2台購入していただく必要があります。 また、ライセンスは同じノード数のものをそれぞれの実IPアドレスで申請していただく必要があります。
- フェイルオーバ機能 (障害時に待機している2台目のFirewallServerに処理を引き継ぐ)のみのサポートです。2台同時に利用できるわけではありません。負荷分散(ロードバランシング)機能はありません。
- 自動フェイルバック時、接続されていたセッションが切断される場合があります。
- 高負荷等の要因により、運用系、待機系の双方で業務が起動してしまう場合があります。その場合、運用系、待機系いずれかのサーバを再起動してください。
- 自動フェイルバックが設定されている場合、運用系サーバ再起動後、自動的に運用系サーバで業務が開始されます。自動フェイルバックが設定されていない場合は、待機系サーバで業務が起動されたままになり、運用系サーバの方が待機状態になります(運用系、待機系の逆転)。運用系サーバに業務を切り替える場合はコマンド(caegrp-m)によりサーバの切り替えを実行する必要があります。